



BASICS OF ETHICAL HACKING

BOEH - Introduzione

K!nd4SUS CyberSecurity Team - Università degli Studi di Milano

A.A. 2025/2026



TABLE OF CONTENTS

1 Risposte al form

- ▶ Risposte al form
- ▶ Struttura del Corso
- ▶ I tutor/lecturer si presentano
- ▶ E dopo BOEH cosa faccio?



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:

- triennale o magistrale di sicurezza
- triennale o magistrale di informatica
- informatica per la comunicazione digitale
- studenti di ITS



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:

- triennale o magistrale di sicurezza
- triennale o magistrale di informatica
- informatica per la comunicazione digitale
- studenti di ITS
- addirittura qualcuno in erasmus in UniMi!



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi
 - ricercatori



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi
 - ricercatori
 - insegnanti



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi
 - ricercatori
 - insegnanti
- Mondo professionale:



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi
 - ricercatori
 - insegnanti
- Mondo professionale:
 - sistemisti



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi
 - ricercatori
 - insegnanti
- Mondo professionale:
 - sistemisti
 - consulenza



DOVE E COSA STUDI/LAUVORI

1 Risposte al form

- Studenti:
 - triennale o magistrale di sicurezza
 - triennale o magistrale di informatica
 - informatica per la comunicazione digitale
 - studenti di ITS
 - addirittura qualcuno in erasmus in UniMi!
- Mondo accademico:
 - dottorandi
 - ricercatori
 - insegnanti
- Mondo professionale:
 - sistemisti
 - consulenza
 - sviluppo



BACKGROUND? CYBERSECURITY|CTF

1 Risposte al form

- “Non ho *ancora fatto niente, vorrei provare*”



BACKGROUND? CYBERSECURITY|CTF

1 Risposte al form

- “Non ho *ancora fatto niente, vorrei provare*”
- “Quasi minimo ma con *voglia di imparare*”



BACKGROUND? CYBERSECURITY|CTF

1 Risposte al form

- “Non ho **ancora fatto niente, vorrei provare**”
- “Quasi minimo ma con **voglia di imparare**”
- “Ho seguito un **corso di crittografia** e ho **fatto alcune challenge** su OverTheWire/Bandit”



BACKGROUND? CYBERSECURITY|CTF

1 Risposte al form

- “Non ho **ancora fatto niente, vorrei provare**”
- “Quasi minimo ma con **voglia di imparare**”
- “Ho seguito un **corso di crittografia** e ho **fatto alcune challenge** su OverTheWire/Bandit”
- “Ho partecipato a olicyber e ho fatto dei corsi pomeridiani a scuola inerenti alle ctf”



BACKGROUND? CYBERSECURITY|CTF

1 Risposte al form

- “Non ho **ancora fatto niente, vorrei provare**”
- “Quasi minimo ma con **voglia di imparare**”
- “Ho seguito un **corso di crittografia** e ho **fatto alcune challenge** su OverTheWire/Bandit”
- “Ho partecipato a olicyber e ho fatto dei corsi pomeridiani a scuola inerenti alle ctf”
- “Ho fatto qualche **challenge di crypto** nelle CTF e ho account per TryHackMe e HackTheBox”



BACKGROUND? CYBERSECURITY|CTF

1 Risposte al form

- “Non ho **ancora fatto niente, vorrei provare**”
- “Quasi minimo ma con **voglia di imparare**”
- “Ho seguito un **corso di crittografia** e ho **fatto alcune challenge** su OverTheWire/Bandit”
- “Ho partecipato a olicyber e ho fatto dei corsi pomeridiani a scuola inerenti alle ctf”
- “Ho fatto qualche **challenge di crypto** nelle CTF e ho account per TryHackMe e HackTheBox”
- “Un partecipante a olicyber [...] **top 100 della classifica**. Ho partecipato alle ultime tre edizione di olicyber 2023, 2024, 2025”



COSA TI ASPETTI DA BOEH? [1]

1 Risposte al form

- Lezione introduttiva, spiegazioni chiare + riferimenti a materiali utili per recuperare le basi/gli argomenti affrontati.



COSA TI ASPETTI DA BOEH? [1]

1 Risposte al form

- Lezione introduttiva, spiegazioni chiare + riferimenti a materiali utili per recuperare le basi/gli argomenti affrontati.
- Una via chiara per iniziare ad esplorare questo mondo



COSA TI ASPETTI DA BOEH? [1]

1 Risposte al form

- Lezione introduttiva, spiegazioni chiare + riferimenti a materiali utili per recuperare le basi/gli argomenti affrontati.
- Una via chiara per iniziare ad esplorare questo mondo
- Capire come si affronta una CTF [...]



COSA TI ASPETTI DA BOEH? [1]

1 Risposte al form

- Lezione introduttiva, spiegazioni chiare + riferimenti a materiali utili per recuperare le basi/gli argomenti affrontati.
- Una via chiara per iniziare ad esplorare questo mondo
- Capire come si affronta una CTF [...]
- Un'occasione per approfondire certi temi e un momento per smanettare su qualcosa di nuovo



COSA TI ASPETTI DA BOEH? [1]

1 Risposte al form

- Lezione introduttiva, spiegazioni chiare + riferimenti a materiali utili per recuperare le basi/gli argomenti affrontati.
- Una via chiara per iniziare ad esplorare questo mondo
- Capire come si affronta una CTF [...]
- Un'occasione per approfondire certi temi e un momento per smanettare su qualcosa di nuovo
- Introduzione e conoscenza di base dei principali campi dell'ethical hacking (crypto, binary, reverse e web)



COSA TI ASPETTI DA BOEH? [2]

1 Risposte al form

- Persone davvero appassionate e tante tante sfide.



COSA TI ASPETTI DA BOEH? [2]

1 Risposte al form

- Persone davvero appassionate e tante tante sfide.
- Vorrei trovare persone con cui discutere di questi argomenti.



COSA TI ASPETTI DA BOEH? [2]

1 Risposte al form

- Persone davvero appassionate e tante tante sfide.
- Vorrei trovare persone con cui discutere di questi argomenti.
- Una bella esperienza di apprendimento di gruppo preparatoria a CTF con l'intenzione di partecipare a tali eventi.



COSA TI ASPETTI DA BOEH? [2]

1 Risposte al form

- Persone davvero appassionate e tante tante sfide.
- Vorrei trovare persone con cui discutere di questi argomenti.
- Una bella esperienza di apprendimento di gruppo preparatoria a CTF con l'intenzione di partecipare a tali eventi.
- Mi aspetto di trovare un ambiente comunicativo e collaborativo, in cui poter imparare attraverso il confronto diretto e l'esperienza pratica.



COSA TI ASPETTI DA BOEH? [3]

1 Risposte al form

- Qualcosa



COSA TI ASPETTI DA BOEH? [3]

1 Risposte al form

- Qualcosa
- Bravi che avete organizzato 🤝



COSA TI ASPETTI DA BOEH? [3]

1 Risposte al form

- Qualcosa
- Bravi che avete organizzato 🤝
- Cose sus immagino



COSA TI ASPETTI DA BOEH? [3]

1 Risposte al form

- Qualcosa
- Bravi che avete organizzato 🤝
- Cose sus immagino
- Sorprendimi



TABLE OF CONTENTS

2 Struttura del Corso

- ▶ Risposte al form
- ▶ Struttura del Corso
- ▶ I tutor/lecturer si presentano
- ▶ E dopo BOEH cosa faccio?



ARGOMENTI E LIVELLO

2 Struttura del Corso

- Il corso sarà introduttivo: livello base e modo di ragionare per affrontare le challenge



ARGOMENTI E LIVELLO

2 Struttura del Corso

- Il corso sarà introduttivo: livello base e modo di ragionare per affrontare le challenge
- Affronteremo diverse macroaree: forensics, crypto, web e binary



ARGOMENTI E LIVELLO

2 Struttura del Corso

- Il corso sarà introduttivo: livello base e modo di ragionare per affrontare le challenge
- Affronteremo diverse macroaree: forensics, crypto, web e binary
- Spoiler: non hackereremo la NASA



ARGOMENTI E LIVELLO

2 Struttura del Corso

- Il corso sarà introduttivo: livello base e modo di ragionare per affrontare le challenge
- Affronteremo diverse macroaree: forensics, crypto, web e binary
- Spoiler: non hackereremo la NASA... per ora 😊
- ... ma magari entro la volta prossima sì dai



CALENDARIO DI MASSIMA

2 Struttura del Corso

- **Andrea:** 13, 15, 20 gennaio (Web)
- **Samuele:** 22, 27, 29 gennaio (Crypto e Forensics)
- **Cristian:** 3, 5, 10 febbraio (Pwn e Rev)
- Discussione dei primi progettini a Marzo



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione bisogna fare un progettino



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione bisogna fare un progettino
- Nulla di troppo elaborato:



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📄 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😎



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📄 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📄 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📄 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge
 - Sviluppo di un tool che possa aiutare per certe famiglie di challenge



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📱 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge
 - Sviluppo di un tool che possa aiutare per certe famiglie di challenge
 - Sempre aperti ad altro!



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📱 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge
 - Sviluppo di un tool che possa aiutare per certe famiglie di challenge
 - Sempre aperti ad altro!
 - Qualcuno hackerà la NASA? 😊



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📄 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge
 - Sviluppo di un tool che possa aiutare per certe famiglie di challenge
 - Sempre aperti ad altro!
 - Qualcuno hackerà la NASA? 😲
- Sceglierete un *tutor* tra noi lecturer che vi seguirà per il progetto



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📱 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge
 - Sviluppo di un tool che possa aiutare per certe famiglie di challenge
 - Sempre aperti ad altro!
 - Qualcuno hackerà la NASA? 🤔
- Sceglierete un *tutor* tra noi lecturer che vi seguirà per il progetto
- Cerchiamo di organizzare una giornata in dipartimento per le esposizioni dei progetti: mini-conferenza!



PROGETTINO

2 Struttura del Corso

- Per ottenere il certificato di partecipazione 📱 bisogna fare un progettino 💻
- Nulla di troppo elaborato:
 - Dimostrazione di un attacco contro un protocollo crittografico 😊
 - Risoluzione (*writeup*) di una challenge più avanzata rispetto a quelle viste a lezione
 - Sviluppo di una nuova (interessante!) challenge
 - Sviluppo di un tool che possa aiutare per certe famiglie di challenge
 - Sempre aperti ad altro!
 - Qualcuno hackerà la NASA? 🤔
- Sceglierete un *tutor* tra noi lecturer che vi seguirà per il progetto
- Cerchiamo di organizzare una giornata in dipartimento per le esposizioni dei progetti: mini-conferenza!
- (per chi è lontano ovviamente faremo online)



UNA CTF FINALE?

2 Struttura del Corso

⚠ NULLA DI UFFICIALE ⚠

Forse parteciperemo tutti insieme alla PicoCTF 2026 (primavera)



TABLE OF CONTENTS

3 I tutor/lecturer si presentano

- ▶ Risposte al form
- ▶ Struttura del Corso
- ▶ I tutor/lecturer si presentano
- ▶ E dopo BOEH cosa faccio?



TOCCA A NOI

3 I tutor/lecturer si presentano

- Samuele Mancossi — Crypto / Forensics



TOCCA A NOI

3 I tutor/lecturer si presentano

- Cristian Salvi — Pwn / Reverse



TOCCA A NOI

3 I tutor/lecturer si presentano

- Andrea Lunghi — Web



TABLE OF CONTENTS

4 E dopo BOEH cosa faccio?

- ▶ Risposte al form
- ▶ Struttura del Corso
- ▶ I tutor/lecturer si presentano
- ▶ E dopo BOEH cosa faccio?



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it
- Sarà organizzato Low Level Nights, un corso simile ma su binary, reverse e hardware!



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it
- Sarà organizzato Low Level Nights, un corso simile ma su binary, reverse e hardware!
- Si può sempre e comunque partecipare alle attività del gruppo!



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it
- Sarà organizzato Low Level Nights, un corso simile ma su binary, reverse e hardware!
- Si può sempre e comunque partecipare alle attività del gruppo!
 - CTF (anche del torneo CyberCup)



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it
- Sarà organizzato Low Level Nights, un corso simile ma su binary, reverse e hardware!
- Si può sempre e comunque partecipare alle attività del gruppo!
 - CTF (anche del torneo CyberCup)
 - Conferenze



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it
- Sarà organizzato Low Level Nights, un corso simile ma su binary, reverse e hardware!
- Si può sempre e comunque partecipare alle attività del gruppo!
 - CTF (anche del torneo CyberCup)
 - Conferenze
 - Eventi



PRIMA O POI BOEH FINISCE 😢

4 E dopo BOEH cosa faccio?

- “*every fair from fair sometime declines*” Sonnet 18, Shakespeare
- CyberChallenge.it
- Sarà organizzato Low Level Nights, un corso simile ma su binary, reverse e hardware!
- Si può sempre e comunque partecipare alle attività del gruppo!
 - CTF (anche del torneo CyberCup)
 - Conferenze
 - Eventi
 - (*anche come organizzatori...*)



Basics Of Ethical Hacking

Thank you for listening!

Any questions?